UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF 2283 MORIAH ROAD, OAK HILL, OHIO	**SW No.** 2:24-mj-118 **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Andrew J. Gafford, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 2283 Moriah Road, Oak Hill, OH, 45656 (hereinafter "PREMISES"), which is the residence of Evan HUNT ("HUNT"), devices controlled by or in the possession of HUNT, including the cell phone(s) in the use and/or possession of HUNT (the "TARGET DEVICE(S)"), and HUNT's person, all further described in Attachment A, for the things described in Attachment B. This warrant authorizes only the search of devices owned and controlled by HUNT and does not authorize the search of devices, including laptop computers or mobile phones, primarily used or controlled by any other residents of the PREMISES.

2. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that statement is described in substance and is not intended to be a verbatim recitation of such statement. Wherever in this affidavit I quote statements, those quotations have been taken from draft transcripts, which are subject to further revision.

3. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I've drawn from my training, experience, and knowledge of the investigation.

AFFIANT BACKGROUND

4. I am Special Agent with the Federal Bureau of Investigation (FBI). I have been a Special Agent with the FBI since February 2011 and am currently assigned to the Joint Terrorism Task Force (JTTF) in the FBI Cincinnati Division, Columbus Resident Agency. I have spent most of my FBI career investigating, managing, and supporting international and domestic terrorism investigations which often involve violations of Title 18 of the United States Code. I have assisted in the preparation of numerous search warrant applications, conducted or participated in physical and electronic surveillance, assisted in the execution of search warrants, debriefed informants and reviewed other pertinent records. Currently, I am tasked with investigating criminal activity in and around the Capitol grounds on January 6, 2021. As such, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1512 (c)(2) (obstruction of Congress); 1752(a)(1) (entering or remaining in restricted buildings or grounds); 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds) and 40 U.S.C. §§ 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings or Grounds) and 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol Building) (the "TARGET

OFFENSES") that have been committed by Evan Hunt ("HUNT" or "the Subject") and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, the Subject, as well as others observed by the Subject. There is also probable cause to search the PREMISES, the Person, and the Property, further described in Attachment A, for the things described in Attachment B.

PROBABLE CAUSE

Background – The U.S. Capitol on January 6, 2021

7. U.S. Capitol Police (USCP), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred on January 6, 2021, at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510.

8. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

9. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, two staircases, and multiple terraces. On the east side of the Capitol is the East Front, which includes three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and closed to members of the public on January 6, 2021.

10. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020

("Certification"). The joint session began at approximately 1:00 p.m. Eastern Standard Time1 in the House of Representatives. Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

11. The grounds around the Capitol were posted and cordoned off, and the entire area as well as the Capitol building itself were restricted as that term is used in Title 18, United States Code, Section 1752 due to the fact that the Vice President and the immediate family of the Vice President, among others, would be visiting and did visit the Capitol complex that day.

12. At around 1:00 p.m., individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol. As a result of these and other similar actions by the crowd, the situation at the Capitol became a civil disorder as that term is used in Title 18, United States Code, Section 231. The civil disorder obstructed the ability of the U.S. Secret Service to perform the federally protected function of protecting Vice President Pence.

13. As they advanced unlawfully onto Capitol grounds and towards the U.S. Capitol building over the next several hours, individuals in the crowd destroyed barricades and metal fencing and assaulted law enforcement officers with fists, poles, thrown objects, and chemical irritant sprays, among other things. Individuals in the crowd carried weapons including tire irons, sledgehammers, bear spray, and tasers, some of which were also used to assault members of law enforcement. A number of individuals in the crowd wore tactical vests, helmets, and respirators.

[1] All times stated in this affidavit are in Eastern Standard Time or Eastern Daylight Time unless otherwise noted.

14. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured.

15. Beginning shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement.

16. Once inside, certain of the unlawful entrants destroyed property, stole property, and assaulted federal police officers.

17. Between approximately 2:10 p.m., and 2:30 p.m., Vice President Pence evacuated the Senate Chamber, and the Senate and House of Representatives went into recess. Unlawful entrants into the U.S. Capitol building attempted to break into the House chamber by breaking the windows on the chamber door. Law enforcement officers inside the House of Representatives drew their weapons to protect members of the House of Representatives who were stuck inside. Both the Senate and the House of Representatives Chamber were eventually evacuated.

18. At around 2:47 p.m., subjects broke into the Senate Chamber not long after it had been evacuated.

19. At around 2:48 p.m., DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m. Mayor Bowser's order imposing a curfew in the District of Columbia impacted interstate commerce. For example, grocery store Safeway closed all 12 of its stores in the District of Columbia as of 4 p.m. that day, and Safeway's stores were supposed to close at 11 p.m.

20. At about 3:25 p.m., law enforcement officers cleared the Senate floor. Between 3:25 and around 6:30 p.m., law enforcement was able to clear the U.S. Capitol of all of the subjects.

21. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening, the joint session could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol throughout the events, including during the time he was evacuated from the Senate Chamber until the joint session concluded at approximately 3:44 a.m. on January 7, 2021.

22. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

23. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

24. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging

and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

Facts Specific to This Application

25. As part of its ongoing investigation into criminal activity on and around the Capitol grounds on January 6, 2021, the FBI sought assistance identifying individuals who entered the Capitol building without authority on January 6, 2021. One individual who entered the Capitol was identified as a white male wearing a black beanie, dark gray jacket, black backpack, and American flag-printed scarf, as shown below.

Figure 1

Figure 2

26. The FBI identified this individual as Evan Hunt (HUNT). The identification of

HUNT is described in detail below. *See* Paragraphs 38-47.

27. Another individual who entered the Capitol was identified as a white male wearing a red and gray Ohio State University jacket, a red baseball cap, blue jeans, black gloves, and a Trump flag styled as a cape. He sometimes, but not always, wore a blue surgical mask, as shown below.

Figure 3

Figure 4

28. The FBI identified this individual as Clayton Hildebrand ("HILDEBRAND").

29. I investigated HUNT's and HILDEBRAND's activities on January 6, 2021. Pursuant to this investigation, I reviewed footage and photographs from January 6, 2021, including publicly available footage, Capitol closed circuit television (CCTV) surveillance footage, and footage obtained during the course of this investigation.

30. In the footage that I reviewed, HUNT and HILDEBRAND can be seen on Capitol grounds and inside of the Capitol building with an individual separately identified as Michael Sposite (SPOSITE). SPOSITE was identified as a white male wearing a green jacket, blue jeans,

a gray and black backpack with a walkie talkie on one strap, and a black and green camouflage hat. HUNT is circled in yellow in Figures 5 through 12, below, HILDEBRAND is circled in red, and SPOSITE is circled in green.

Figure 5

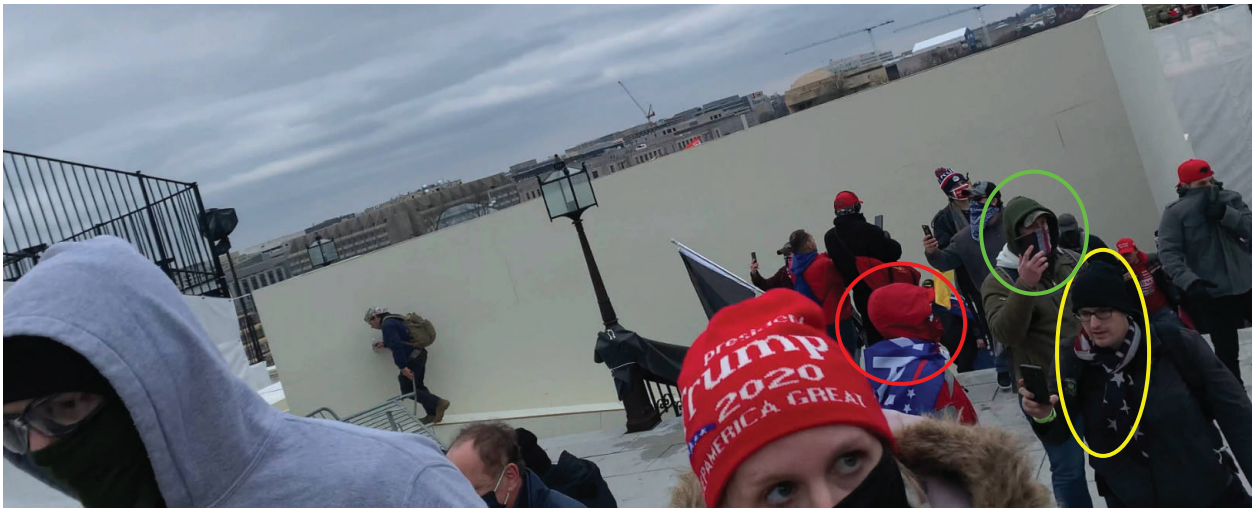

Figure 6

Figure 7

31. HUNT, SPOSITE, and HILDEBRAND were among the first rioters to approach the West Front of the Capitol building. Figures 8 and 9 below show HUNT, SPOSITE, and HILDEBRAND near the initial breach point on the West side of the Capitol. Based on my training and experience, it appears that this footage was taken prior to the initial breach of the West Front of the Capitol building.

Figure 8

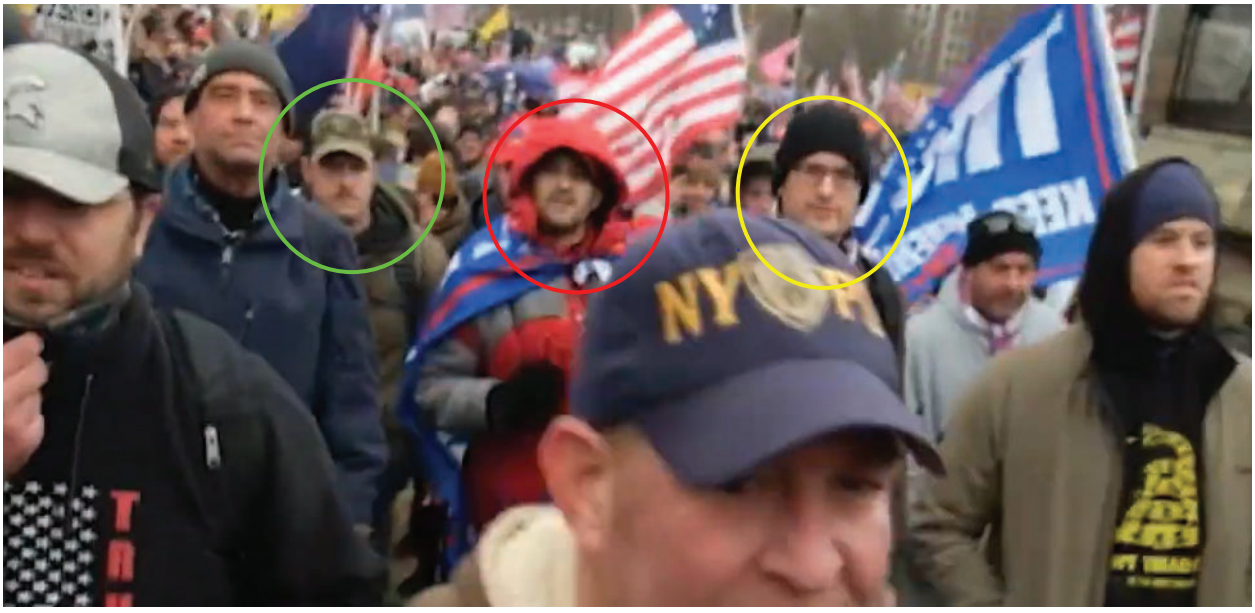

Figure 9

32. After moving past the initial breach point and entering restricted Capitol grounds, HUNT, HILDEBRAND, and SPOSITE remained on the West Front of the Capitol building. Figures 10-12 below show HUNT and HILDEBRAND engaged in the riot within the restricted Capitol grounds.

Figure 10

Figure 11

Figure 12

33. As shown in Figure 11, above, HUNT and HILDBRAND were exposed to tear gas, pepper spray, or some other chemical irritant while on the West side of the Capitol building. During an interview with the FBI, HILDEBRAND stated that he was exposed to pepper spray on January 6, 2021 but not sprayed directly.

34. The footage that I reviewed also indicates that HUNT, HILDEBRAND, and SPOSITE watched while another rioter used a knife to cut a tarp covering scaffolding on the lower West Plaza of the Capitol building. Based on my investigation, HUNT, HILDEBRAND, and SPOSITE were also in the vicinity of violent interactions between other rioters and law enforcement officers.

35. HUNT, HILDEBRAND, and SPOSITE entered the Capitol building through the Senate Wing Doors, adjacent to the Upper Northwest Terrace of the building, at approximately 2:17 p.m. EST, as shown in Figure 13, below. HUNT is again circled in yellow, HILDEBRAND is circled in red, and SPOSITE is circled in green in Figures 13 through 17.

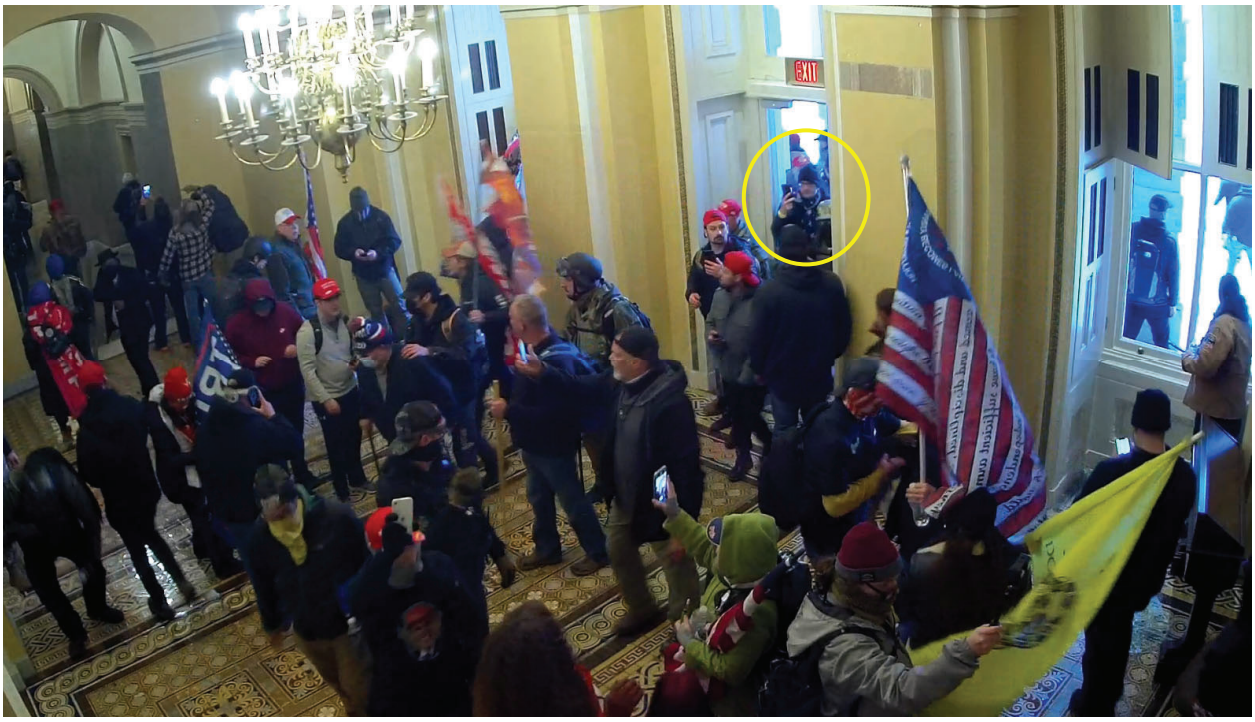

Figure 13

Figure 14

36. After entering the building, HUNT, HILDEBRAND, and SPOSITE turned right, towards the South side of the building. *See* Figures 15 and 16.

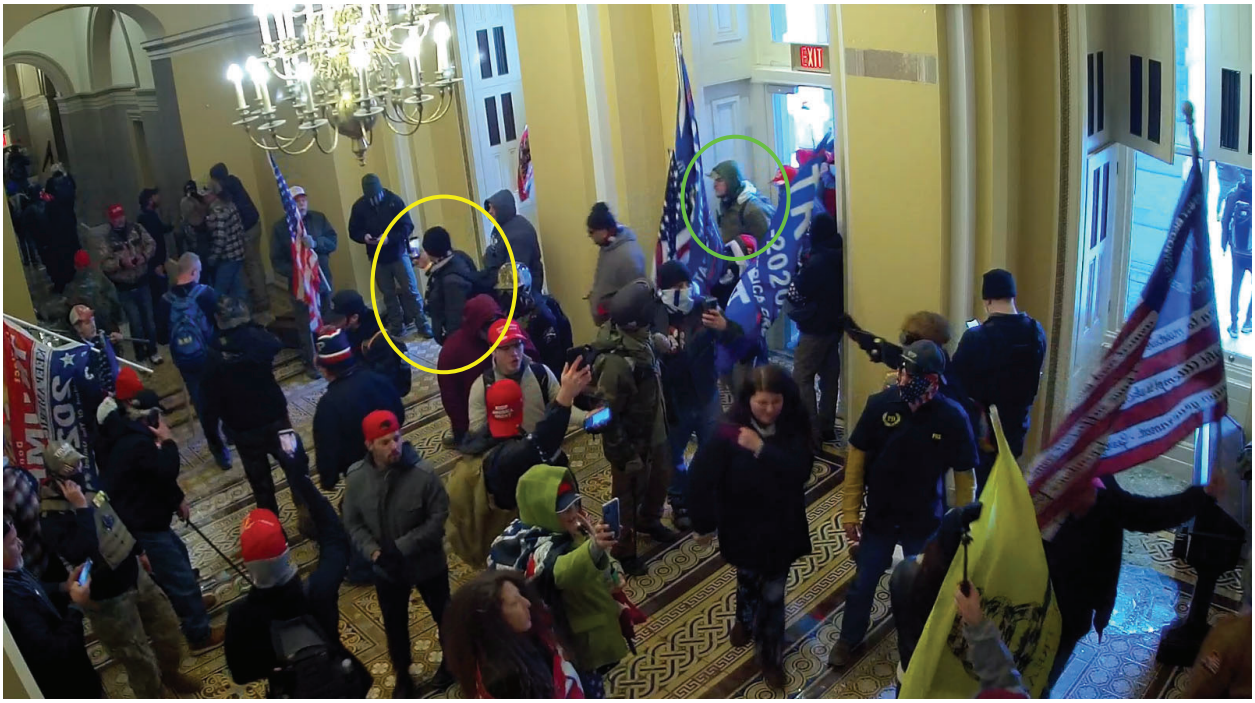

Figure 15

Figure 16

37. HUNT, HILDEBRAND, and SPOSITE exited the building through the same door through which they entered approximately three minutes later, at around 2:20 p.m. EST, as shown in Figure 17.

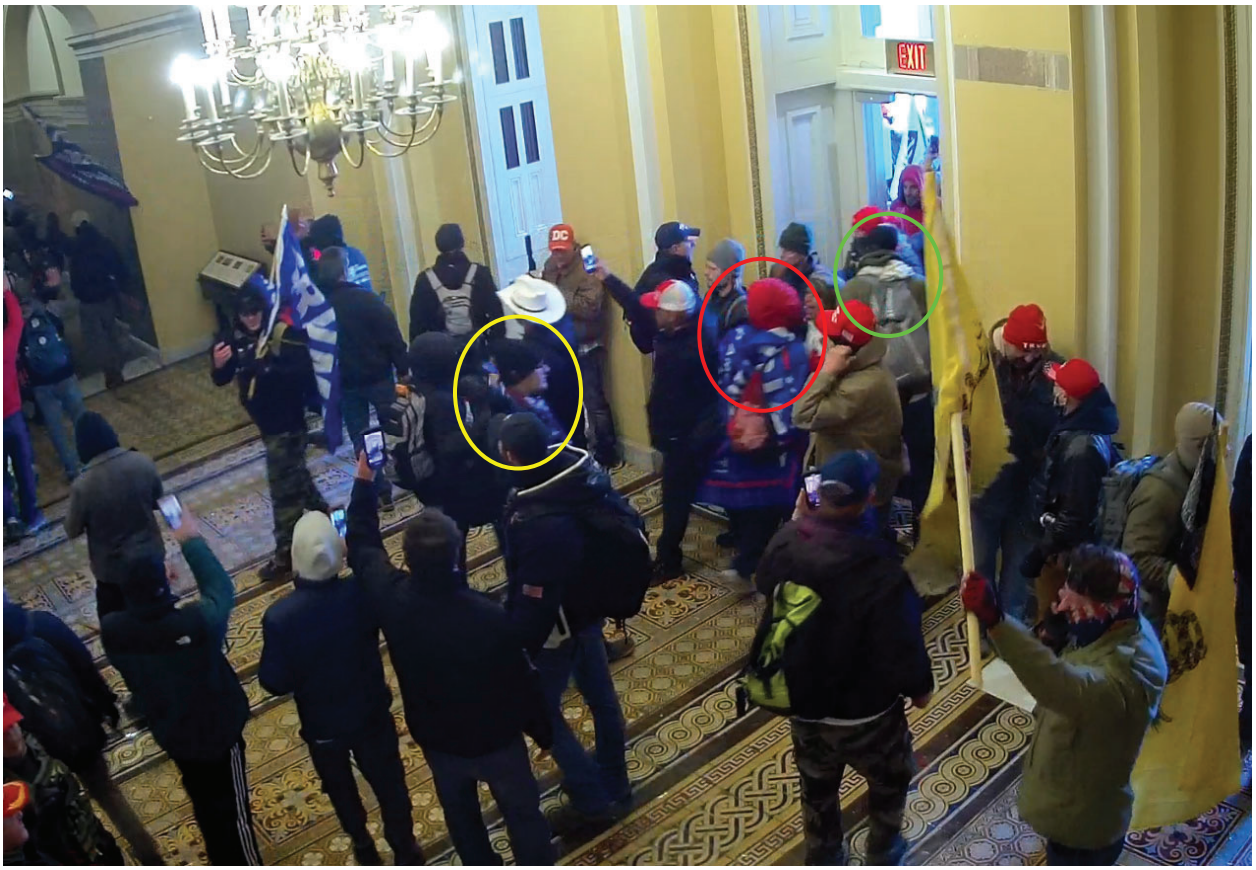

Figure 17

Identification of Evan HUNT

38. As part of its ongoing investigation into criminal activity on and around the Capitol grounds on January 6, 2021, including the identification of individuals who entered the U.S. Capitol without authority, the FBI compared photographs of individuals inside of the U.S. Capitol on January 6, 2021 against archived open-source footage. Pursuant to that process, the FBI reviewed a photograph of several individuals at a political rally in Ohio on or about June 26, 2021.

39. In or around August 2022, the FBI compared that photograph to Capitol surveillance footage and other footage from January 6, 2021, and determined one individual in the photograph, SUBJECT 1, was inside the U.S. Capitol on January 6, 2021 with two other individuals already known to the FBI – SPOSITE and HILDEBRAND. The individual identified as SUBJECT 1 at that time is depicted below in an excerpt from the photograph from the June 26,

2021 rally.

Figure 18

40. On August 22, 2022, the FBI interviewed a tipster (TISPTER 1) as part of an investigation into another individual suspected of criminal activity on January 6, 2021.

41. When shown a photograph of SUBJECT 1, TIPSTER 1, HUNT's former co-worker, identified SUBJECT 1 as Evan HUNT of Columbus, Ohio. At a later date, I showed TIPSTER 1 Figure 1, above, showing HUNT on restricted Capitol grounds on January 6, 2021. TIPSTER 1 also positively identified HUNT in that image.

42. TIPSTER 1 also provided a Facebook account for HUNT. The FBI then searched law enforcement databases for "Evan Hunt" and identified an Ohio driver's license photo which FBI personnel believed matched the photo of HUNT from the June 2021 rally in Ohio. An image from the Facebook account identified by TIPSTER 1 is below.

Figure 19

43. The FBI subsequently searched for and compared images of HUNT against footage from January 6, 2021, including open-source footage and CCTV footage. The queries yielded several photos of HUNT both outside and inside the U.S. Capitol building on January 6, 2021. *See, e.g.*, Figures 10-12 and 13-17 above.

44. I compared the above images to HUNT's driver's license photograph and images from HUNT's Facebook account. Based on that comparison, I positively identified the individual depicted by the yellow circle in Figures 10-12 and 13-17 above as HUNT.

45. Investigation into HUNT revealed that he was present at the Capitol throughout the day on January 6, 2021 with SPOSITE and HILDEBRAND, both of whom had been previously identified by the FBI.

46. During an interview with the FBI, HILDEBRAND provided the FBI with video footage that he took from inside of the Capitol building. In two of the video clips provided by HILDEBRAND, the person taking the video can be heard yelling, "Evan!" Screenshots from the footage provided by HILDEBRAND are below (Figures 20 and 21).

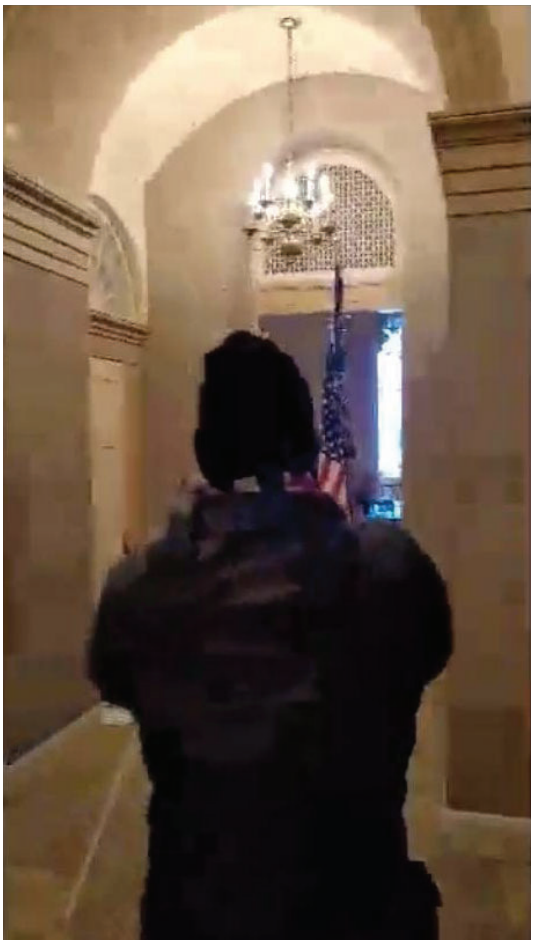

Figure 20

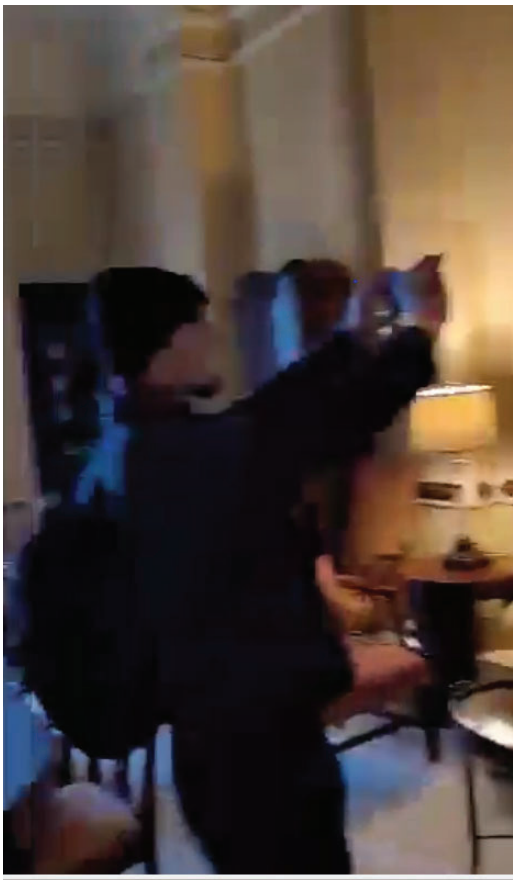

Figure 21

47. I compared these videos with other footage of HUNT from January 6, 2021 and determined that the individual in Figures 20 and 21 is HUNT, based on his attire and general appearance.

HUNT's Facebook Profile

48. As part of my investigation into HUNT, I reviewed HUNT's public Facebook profile, *see also* Paragraph 42, as well as content lawfully received from Meta Platforms, Inc. from HUNT's Facebook profile.

49. HUNT regularly used his Facebook in the months leading up to January 6, 2021. His posts and communications prior to January 6, 2021 demonstrate his knowledge about the electoral process and the electoral vote scheduled for January 6, 2021. The information received relevant to HUNT's Facebook also indicates that HUNT traveled to Washington, D.C. with the

intent to obstruct or impede the electoral vote.

50. For example, on December 22, 2020, HUNT posted a status on Facebook which stated in part: "if you can try in any way, be in Washington DC on Jan. 6 and be LOUD that We The People will not surrender our Republic to this fraud and tyranny they are trying to put us under." The next day, on December 23, 2020, HUNT commented on a post stating in part: "I'm still looking to the electoral college vote on the 6th…I'll be in DC on the 6th for the peaceful protest to show our government that the people will not accept these fraudulent electors…." That same day, HUNT commented on another Facebook user's photograph stating in part: "I am convinced we need to fight to make sure this election is not stolen…I will be in DC on Jan 6…." And on December 29, 2020, HUNT posted a status stating: "Patriots have had enough. To those who are 'just doing their job,' if you enforce this garbage, you are committing TREASON against We The People and we have a right and a duty to fight back!" There are several other posts in addition to the ones summarized here that also confirm HUNT's knowledge of the electoral process and his intent to travel to Washington, D.C. to obstruct that process.

Probable Cause that Evidence Will be Found on HUNT's Digital Devices

51. Multiple images from January 6, 2021 show HUNT holding a cell phone. *See, e.g.*, Figure 22 (HUNT holding a cell phone in his hand while walking towards the Capitol building) and Figure 23, below (HUNT holding a cell phone in his hand near the initial breach point on the West side of the Capitol grounds).

Figure 22

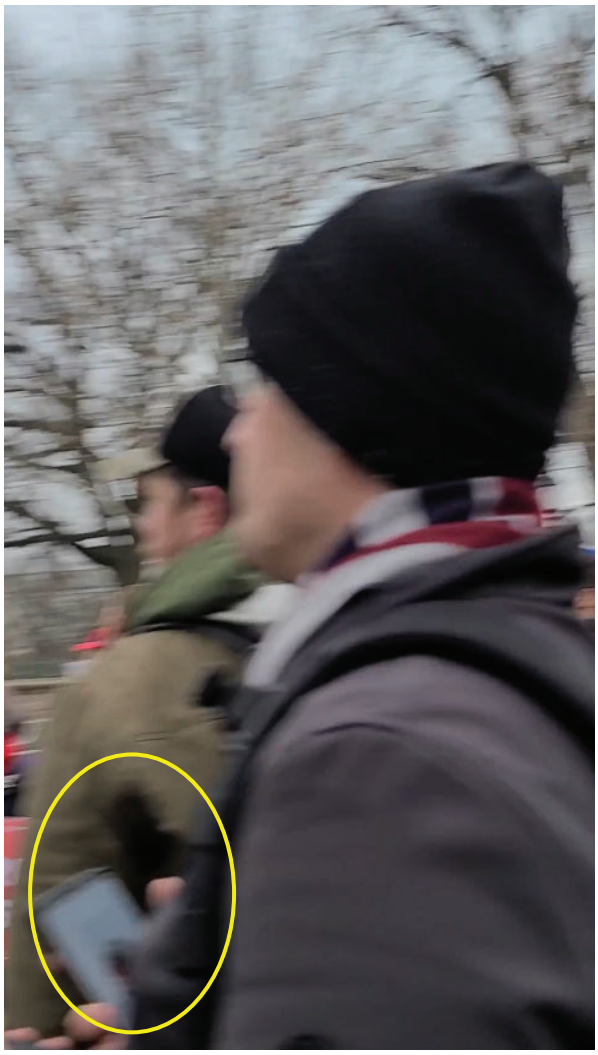

Figure 23

52. Based on my training and experience and on the position in which HUNT is holding that cell phone, he likely used his phone to record video footage and/or take photographs throughout the day on January 6, 2021.

53. In particular, my review of the CCTV footage from inside of the Capitol building indicates that HUNT likely used his cell phone to film video footage as he walked through the building. CCTV footage captured as HUNT entered the building shows that he held his phone up around shoulder height as he entered the building and soon after he entered, in a position that I recognize as consistent with someone who is filming their surroundings. *See, e.g.,* Figures 24-25.

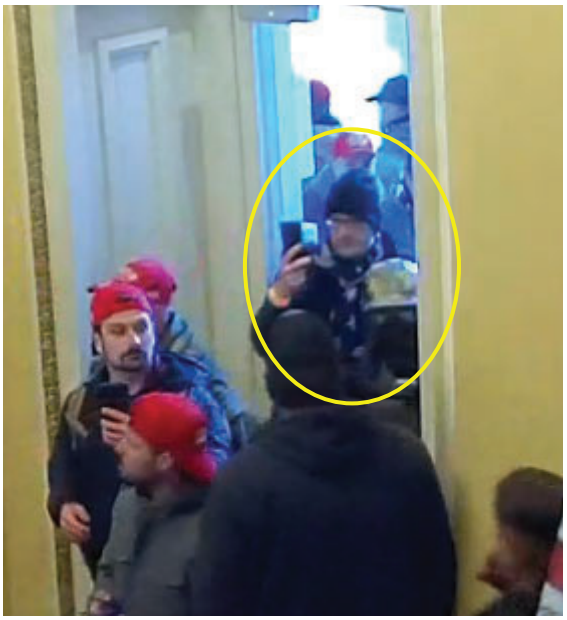

Figure 24

Figure 25

54. Footage captured as HUNT turned South indicates that his cell phone was turned on and the camera on his cell phone was open as he walked through the building:

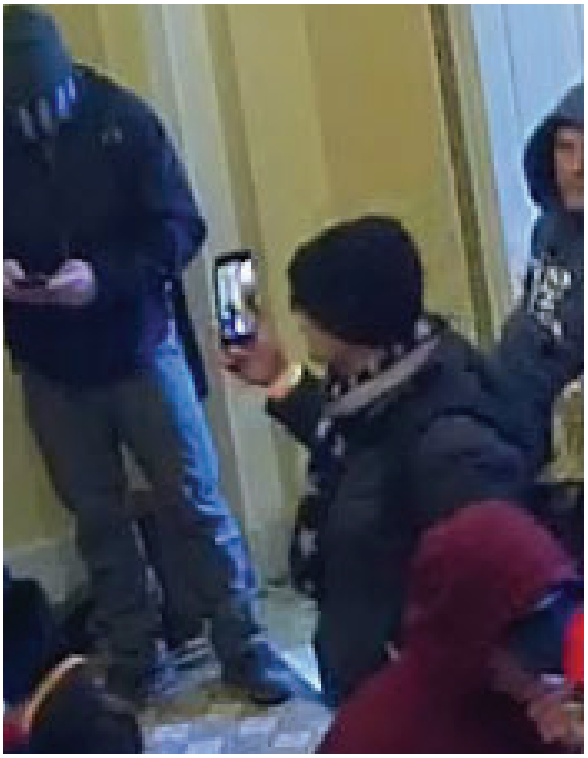

Figure 26

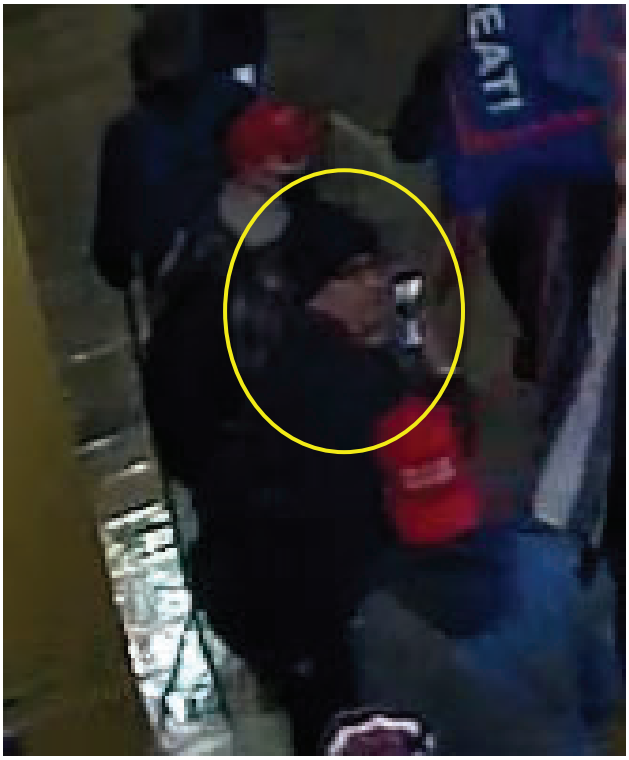

Figure 27

55. Further, the video footage collected from HILDEBRAND also appears to show HUNT taking photographs of his surroundings. In the screen capture from that footage below, for instance, HUNT is standing in a room to the South of Senate Wing Doors with his phone above shoulder height in a position that, in my training and experience, suggests he is taking a photograph. *See* Figure 28. Another screen capture from that same video clip shows him holding his phone outstretched towards the wall. *See* Figure 29 (HUNT's arms circled in yellow).

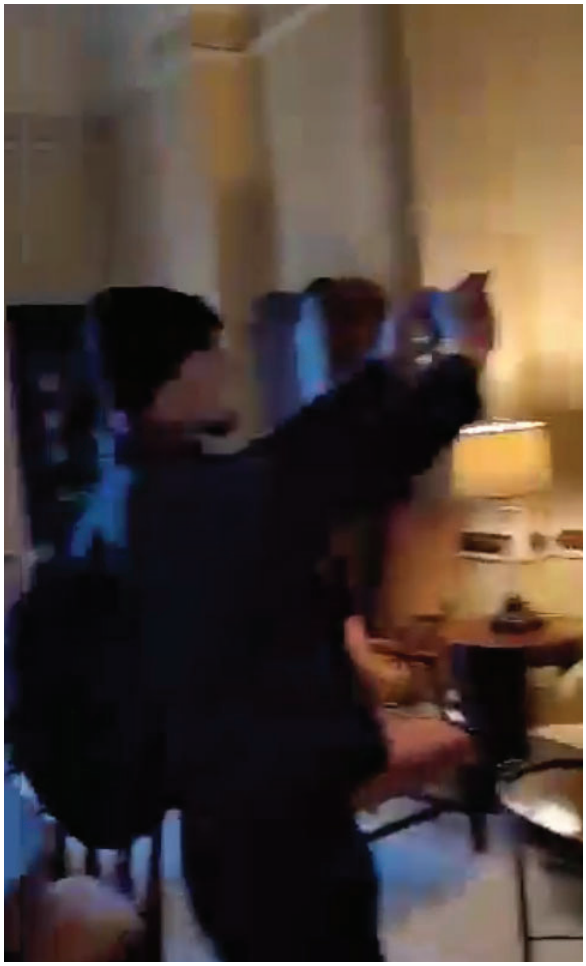

Figure 28

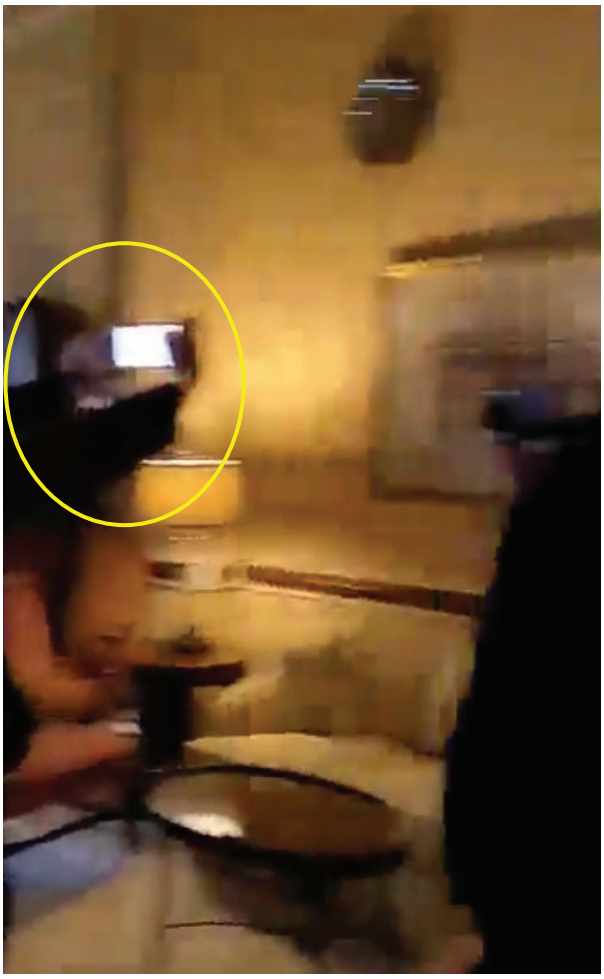

Figure 29

56. In addition, other footage from January 6, 2021 appears to show HUNT holding a recording device. In my training and experience, this device is likely a GoPro or a similar device. This device is circled in yellow in Figures 30-32.

Figure 30

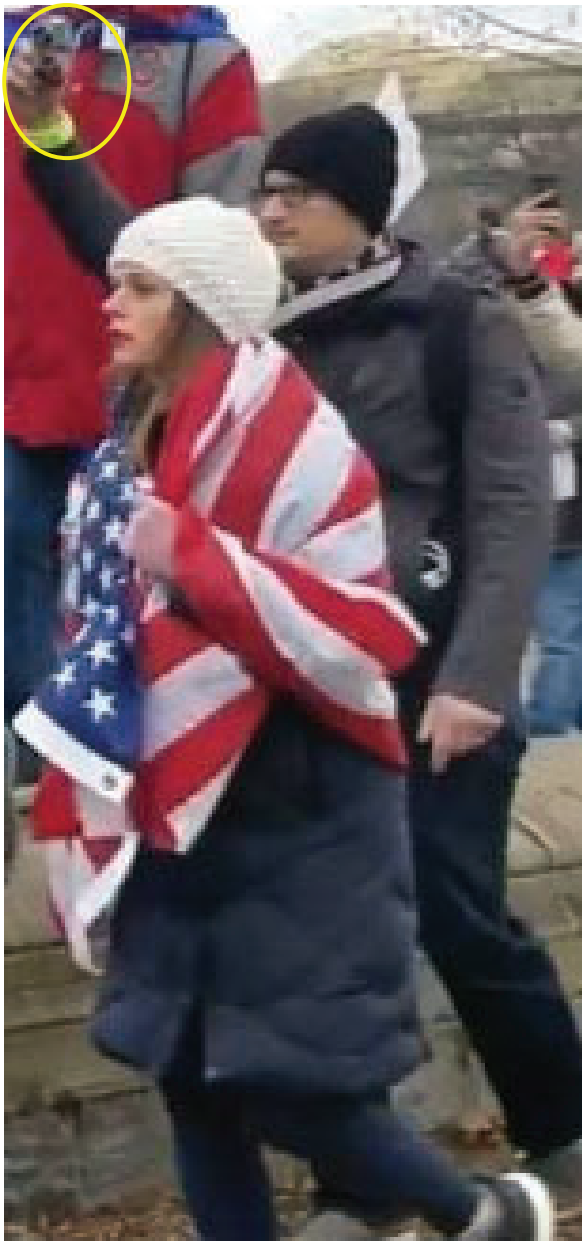

Figure 31

Figure 32

57. Video footage and images from January 6, 2021 would be relevant to the TARGET OFFENSES, as would be communications stored on HUNT's cell phone, such as text messages or messages from other social media or messaging platforms.

58. Database and open-source checks performed by the FBI indicated that HUNT's cell phone number is 614-535-5095. I served a subpoena on T-Mobile requesting account records on January 9, 2023. The returns received from T-Mobile confirmed that the number 614-535-5095 is an active account registered to HUNT as of the time that I received those returns. HUNT also updated his driver's license records with the Ohio Bureau of Motor Vehicles in October 2023, at which time he self-reported his phone number as that same phone number.

59. There is probable cause to believe that HUNT used his cell phone to communicate, including to send messages via text message and/or social media platforms, on January 6, 2021 and in the days leading up to and following January 6, 2021. For instance, I know that HUNT frequently communicated via Facebook about the January 6, 2021 riot and the 2020 Presidential Election. In my training and experience, individuals who are active on Facebook frequently use the "Facebook Messenger" application on their cell phones to communicate with one another. If an individual uses that application, those messages may be stored within the application on that individual's cell phone. Furthermore, records received from T-Mobile also confirmed that HUNT used his cell phone throughout the day on January 6, 2021: according to the data received, he received or made approximately 130 calls on January 6, 2021 alone. The data also indicates that he sent and/or received multiple text messages on January 5, 2021 and January 6, 2021.

60. Additionally, based on the investigation, numerous persons who committed the TARGET OFFENSES possessed digital devices to communicate with other individuals to plan their attendance in Washington D.C. on January 6, 2021, to coordinate with other participants at the gatherings there that day, and to communicate and post on social media and digital forums about the events of January 6 after they occurred. I know that HUNT stayed with two other individuals, SPOSITE and HILDEBRAND, throughout the day on January 6, 2021. Based on my training an experience and my review of the evidence, it is likely that he coordinated with SPOSITE and HILDEBRAND prior to January 6, 2021 and/or discussed the events with them afterwards. Indeed, as explained above, *see* Paragraph 58, the records received from T-Mobile confirm that HUNT used his phone throughout the day on January 6, 2021.

61. Searches of cell phones recovered from many individuals arrested in connection with the January 6, 2021 riot have recovered messages, pictures, and other data relevant to January

6, 2021. For example, on February 2, 2024, a search of a defendant's cell phone in the Northern District of Ohio recovered photographs of the defendant at the Capitol on January 6, 2021. Further, on July 28, 2023, a search of a defendant's phone in the Southern District of Ohio yielded pictures, geolocation information and text messages pertaining to the January 6th riot. On June 28, 2023, a search of a defendant's phone in the Eastern District of Missouri recovered photos and videos taken on January 6, 2021. And on April 12, 2023, a search in the District of New Mexico recovered a defendant's phone containing messages, chats, images, audio records, and pdf documents relevant to January 6, 2021

62. I also know, based on my training and experience, that cell phones are expensive, and people routinely retain their cell phones for many months or years. Therefore, even if HUNT has obtained a new cell phone since January 6, 2021, it is likely that his old cell phone will still be found on the PREMISES.

63. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. I also know, for instance, that T-Mobile account holders – such as HUNT – can easily transfer data from one cell phone to another. Thus, there is reason to believe that evidence of the offense that originally resided on the Subject's cell phone may also be saved to other digital devices within the PREMISES.

64. The evidence that I reviewed also indicates that HUNT used a GoPro or another similar recording device on January 6, 2021. *See* Paragraph 56. Based on my training and experience, I know that users of recording devices most frequently upload the footage that they recorded to an external device, such as a laptop computer.

65. Based on the above, there is probable cause to believe that HUNT used his phone throughout the day on January 6, 2021, including while he was on restricted Capitol grounds and within the Capitol building. There is also probable cause to believe that evidence relevant to the TARGET OFFENSES will be saved on other electronic devices found on the PREMISES.

66. The property to be searched includes laptop computers, mobile phones, and/or tablets owned, used, or controlled by HUNT, including but not limited to the TARGET DEVICE(S). For clarity, this warrant does not authorize the search of laptop computers, mobile phones, and/or tablets primarily used or controlled by any person other than HUNT, including by any other residents of the PREMISES.

Probable Cause that Evidence Will Be Found on the PREMISES

67. Based on my training and experience, it is likely that evidence of the TARGET OFFENSES, including the clothing that HUNT wore on January 6, 2021 and the items that he carried with him, will be present on the PREMISES. Items found on the PREMISES are likely to be relevant to this investigation, including as evidence of HUNT's participation in the riot and state of mind in committing the TARGET OFFENSES.

68. There is probable cause to believe that HUNT lives at the PREMISES. In January 2023, the FBI conducted law enforcement database searches of HUNT's identifiers and determined that in October 2023, HUNT obtained a new driver's license under the following address: 2283 Moriah Rd, Oak Hill, Ohio 45656. Based on a review of content lawfully received from Meta Platforms, Inc. from HUNT's Facebook profile, between on or about January and August 2023, HUNT sent multiple Facebook messages in which he stated that he and his family planned to and/or had moved to Oak Hill and/or Jackson County, Ohio. In late January 2024, the FBI conducted spot check surveillance of HUNT's address and confirmed the Sportsmen trailer

pictured in Attachment A was parked on the property at the PREMISES.

69. There is also probable cause to believe that clothing, digital devices, and other items relevant to the TARGET OFFENSES will be found at the PREMISES, even though HUNT has moved to a new residence since the time of those offenses. I know, based on my training and experience, that people routinely re-wear clothing and accessories, store these items in their homes, and keep them for an extended period. Clothing and accessories consistent with those worn by HUNT on January 6, 2021 constitute evidence of the commission of the offenses discussed herein, in that HUNT can be visually identified as the individual in the photos and videos discussed above, in part through the distinct attire and accessories worn that day. I also know that people tend to take many items with them when they move, including clothes and expensive digital devices, such as laptop computers and/or recording devices like GoPros.

70. Some of the items that HUNT wore on January 6, 2021 are distinctive. For instance, he wore a scarf with an American flag pattern on it, as shown above. *See, e.g.*, Figure 30. It also appears that both he and SPOSITE wore walkie-talkies. *See, e.g.*, Figures 1 and 5.

71. Furthermore, as stated above, HUNT appears to have used a recording device to film his surroundings on January 6, 2021. I know, based on my training and experience, that most people store their electronics, including recording devices, computers, tablets, and/or old cell phones, at their homes. It is likely that these devices will be present on the PREMISES.

72. I also know that hundreds of people have been arrested in connection to the riot that occurred at the U.S. Capitol on January 6, 2021. During searches of many of those people's homes, from early 2021 through present, in multiple jurisdictions, law enforcement has recovered clothing, paraphernalia, tools, and devices that were worn, used, or carried on January 6, 2021. Searches of those devices continue to recover information and data relevant to January 6, 2021.

73. For example, on July 31, 2023, a search of a home in the Southern District of Ohio uncovered clothing worn on January 6, 2021 and a cell phone containing relevant messages and photographs. On February 1, 2023, the homes of two suspected rioters were searched in the Eastern District of Michigan. In one home, investigators located clothing worn by the individual at the Capitol on January 6. In the other home, agents discovered both clothing as well as the stick/club this individual took into the Capitol and a protest sign he displayed that day. Additionally, on November 13, 2023, a search of another home in the Eastern District of Michigan recovered a jacket and backpack worn by the defendant to the Capitol on January 6, 2021. On November 21, 2023, a search of a home in the Northern District of Ohio recovered a jacket worn on January 6, 2021, as well as Bluetooth speaker that the defendant carried with him. On December 12, 2023, a search in the Eastern District of Tennessee recovered gloves, a hoodie, and a backpack worn on January 6, 2021. On December 13, 2023, a search in the Northern District of West Virginia recovered a camouflage Washington Capitols jersey and two hats worn on January 6, 2021. And on December 15, 2023, a search in the Eastern District of California recovered a flag worn by the defendant on January 6, 2021, and a cell phone with pictures taken by the defendant at the Capitol building.

TECHNICAL TERMS

74. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part

through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or

locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the

Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running

compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the

name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

75. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers,

mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, such as the TARGET OFFENSES described herein, use digital devices, like the Device(s), to communicate with co-conspirators and associates via multiple platforms, including via text message or other "Short Message Service" ("SMS") messages, email, and social media platforms.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using

readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

76. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

77. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of

particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital

device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

78. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting,

in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

BIOMETRIC ACCESS TO DEVICE(S)

79. This warrant permits law enforcement agents to obtain from the person of EVAN HUNT (but not any other individuals present at the PREMISES at the time of execution of the

warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

80. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

81. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

82. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes

and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

83. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

84. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

85. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data

contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

86. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

87. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s)

to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

88. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION

89. I submit that this affidavit supports probable cause for a warrant to search the PREMISES, Property, and Person described in Attachment A, and to seize the items described in Attachment B.

Respectfully submitted,

Andrew J. Gafford
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on March 4, 2024.

Kimberly A. Johnson
United States Magistrate Judge